1046-D1-1127 **Tamara B Veenstra*** (tamara_veenstra@redlands.edu), 1200 E. Colton Avenue, Mathematics Department, University of Redlands, Redlands, CA 92373. *The Vigenere Cipher: A historical cipher with a modern day application.* Preliminary report.

I have taught a wide variety of courses involving the mathematics of cryptography. These range from an introductory general audience course to an upper level course for mathematics majors. I will provide a brief summary of topics covered in each of these courses. Then I will discuss the historical Vigenere cipher that involves some interesting topics in probability (combinations and permutations) and statistics (frequency analysis of different types of cipher and plain text) to attack this cipher. I will also present how this corresponds to the modern day binary stream ciphers. If time remains I will discuss the connection between linear feedback shift registers, which can be used to generate stream ciphers and special types of polynomials over finite fields. (Received September 14, 2008)